

令和2年及び令和3年の 個人情報保護法改正概要

中央大学国際情報学部
教授 石井 夏生利

令和2年個人情報保護法改正

佐脇紀代志『一問一答 令和2年改正個人情報保護法』（商事法務、2020年）
個人情報保護委員会「個人情報保護法の令和2年改正について」
(https://www.iwsec.org/pws/2020/Images/20210312_PWS2021Meetup_ppc.pdf)
同「令和2年改正個人情報保護法について」内の各情報
(<https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#kentou>)をもとに作成

背景

- 平成27年改正個人情報保護法に設けられた「いわゆる3年ごと見直し」に関する規定（附則第12条）に基づき、個人情報保護委員会において、関係団体・有識者からのヒアリング等を行い、実態把握や論点整理等を実施。
- 自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点から、今般、個人情報保護法の改正を行い、以下の措置を講ずることとしたもの。

2015年改正法附則

第12条

1 略

2 政府は、この法律の施行後3年を目途として、個人情報保護に関する基本方針の策定及び推進その他の個人情報保護委員会の所掌事務について、これを実効的に行うために必要な人的体制の整備、財源の確保その他の措置の状況を勘案し、その改善について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。

3 政府は、前項に定める事項のほか、この法律の施行後3年を目途として、個人情報保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、新個人情報保護法の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。

1 個人の権利の在り方①

- 利用停止・消去等の個人の請求権について、不正取得等の一部の法違反の場合に加えて、個人の権利又は正当な利益が害されるおそれがある場合にも拡充する。
- 保有個人データの開示方法(現行、原則、書面の交付)について、電磁的記録の提供を含め、本人が指示できるようにする。
- 個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする。

利用停止等(改正法第30条第5項)

- 現行法に加えて、① 利用する必要がなくなった場合、② 重大な漏えい等が発生した場合、③ 本人の権利又は正当な利益が害されるおそれがある場合にも拡充
- ③の例
 - ✓ダイレクトメールの送付を受けた本人が、送付の停止を求める意思を表示したにもかかわらず、個人情報取扱事業者がダイレクトメールを繰り返し送付していることから、本人が利用停止等を請求する場合
 - ✓個人情報取扱事業者が、法第23条第1項に違反して第三者提供を行っており、本人を識別する保有個人データについても本人の同意なく提供されるおそれがあることから、本人が利用停止等を請求する場合
 - ✓個人情報取扱事業者が、退職した社員の情報を現在も自社の社員であるようにホームページ等に掲載し、これによって本人に不利益が生じていることから、本人が利用停止等を請求する場合
- ③の解釈
 - ✓一般人の認識を基準として、客観的にみて侵害されるおそれがあること

第三者提供記録の開示請求(改正法第28条5項)

- 第三者提供記録の開示は、本人の同意に基づく場合と、オプトアウト規定に基づく場合の両方が対象
- 第三者提供記録の秘密保持契約を結んでいても、必ずしも不開示情報には該当しない。

1 個人の権利の在り方②

- 6ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象とする。
- オプトアウト規定(※)により第三者に提供できる個人データの範囲を限定し、①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外とする。

(※)本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

オプトアウト(改正法第23条2項及び3項)

①不正取得されたデータ

個人が不正に持ち出した名簿をオプトアウト事業者が取得して提供する場合

②オプトアウトによって提供された個人データ

オプトアウト届出を行っている名簿業者間で名簿交換等を行い、個人データが流通している場合

2 事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。

（※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。

- **違法又は不当な行為を助長する等の不適正な方法**により個人情報を利用してはならない旨を明確化する。

漏えい報告(規則第6条の2～第6条の5)

- ①要配慮個人情報、②財産的被害が発生するおそれがある場合、③不正アクセス等故意によるもの、④1,000人を超える漏えい等
- 速報：事態の発生を認識した後、速やかに速報を求める
- 確報：30日(不正アクセス等の場合は60日)以内

違法又は不当な行為を助長し、又は誘発するおそれがある方法(改正法第16条の2)

- ① 違法な行為を営むことが疑われる業者からの突然の接触によって、本人の平穏な生活を送る権利が侵害されるおそれが想定されるにもかかわらず、当該違反業者に当該本人の個人情報を提供すること
- ② 裁判所による公告等により散在的に公開されている個人情報について、当該個人情報に係る本人に対する差別が、不特定多数の者によって誘発されるおそれがあることが十分に予見できるにもかかわらず、それを集約してデータベース化し、インターネット上で公開すること
- ③ 暴力団員により行われる暴力的要求行為等の不当な行為や総会屋による不当な要求を助長し、又は誘発するおそれが予見できるにもかかわらず、事業者間で共有している暴力団員等に該当する人物を本人とする個人情報や、不当要求による被害を防止するために必要な業務を行う各事業者の責任者の名簿等を、みだりに開示し、又は暴力団等に対しその存在を明らかにすること。

3 事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

（※）現行の認定団体は、対象事業者のすべての分野（部門）を対象とする。

4 データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する。
- 提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。

仮名加工情報(第2章9項、10項、第4章第2節関係)

- 「仮名加工情報」として加工すれば、個人情報に該当しても、
以下の義務は適用除外
 - ✓利用目的の変更の制限(第15条2項)
 - 本人を識別しない、内部での分析・利用であることを条件に(第35条の2、6項～8項)、**新たな目的で利用が可能**
 - ✓漏えい等の報告等(第22条の2)
 - ✓開示・利用停止等の請求対応(第27条～第34条)
- **作成元の「個人情報」は残したまま、これまで通り利用可能**

加工基準(規則第18条の7)

- ①氏名等の特定の個人を識別できる記述等、②個人識別符号、
③財産的被害が生じるおそれのある記述等 の削除・置換



- ①氏名を仮IDに置換、② 旅券番号、マイナンバーを削除、
③ クレジットカード番号を削除

想定事例

1. 当初の利用目的には該当しない目的や、該当するか判断が難しい新たな目的での内部分析
 - ① 医療・製薬分野等における研究
 - ② 不正検知・売上予測等の機械学習モデルの学習等
2. 利用目的を達成した個人情報について、将来的に統計分析に利用する可能性があるため、仮名加工情報として加工した上で保管

個人関連情報

- 氏名と結びついていないインターネットの閲覧履歴、位置情報、クッキー等 *提供先で個人データとなることが想定される場合のみ
× 個人情報、× 仮名加工情報、× 匿名加工情報
- 第三者によって個人データとして取得されることが、通常想定できる場面に確認義務が生じる。当該第三者との取引環境等の客観的事情に照らし、一般人の認識を基準として判断。
 - *個人関連情報を提供する際、提供先において当該個人関連情報を氏名等と紐付けることができる固有ID等を併せて提供する場合など
 - *提供先第三者との間で「個人関連情報を個人データとして取得しない」旨の契約を締結している場合は、通常想定できる場面には該当しない。但し、提供先第三者が多数の顧客情報を有する大規模通販事業者である場合等は、個人関連情報と容易に照合できる顧客情報等を当該第三者が保有していないことを確認することが望ましい。

提供元の記録義務(規則第18条の4、第18条の5)

- ①提供年月日、②第三者の氏名等、③個人関連情報の項目等の記録
- 原則3年の保存

5 ペナルティの在り方

- 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる。**

(※)命令違反：6月以下の懲役又は30万円以下の罰金 → 1年以下の懲役又は100万円以下の罰金 虚偽報告等：30万円以下の罰金 → 50万円以下の罰金

- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引き上げる**(法人重科)。

(※)個人と同額の罰金(50万円又は30万円以下の罰金) → 1億円以下の罰金

改正前後の法定刑の比較

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会□からの命令への違反	行為者	6月以下	1年以下	30万円以下	100万円以下
	法人等	-	-	30万円以下	1億円以下
個人情報データベース等の不正提供等	行為者	1年以下	1年以下	50万円以下	50万円以下
	法人等	-	-	50万円以下	1億円以下
個人情報保護委員会□への虚偽報告等	行為者	-	-	30万円以下	50万円以下
	法人等	-	-	30万円以下	50万円以下

個人情報保護委員会「令和2年 改正個人情報保護法について」
<https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#kentou>

6 法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって 担保された報告徴収・命令の対象**とする。
命令に従わない場合の公表 *国内事業者も対象
- 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

外国にある第三者への提供制限(規則第11条の3、第11条の4)

- 本人同意：同意取得時の情報提供
 - ✓①移転先の所在国名、②適切かつ合理的な方法で確認された当該国の個人情報保護制度、③移転先が講ずる措置
- 基準に適合する体制を整備した事業者：「必要な措置」及び本人の求めに応じて情報提供
 - ✓①移転先における個人データの取扱状況及びそれに影響を及ぼしうる移転先の所在国の制度の有無の定期的な確認、②適正な取扱いに問題が生じた場合の対応(適正な取扱いの継続的な確保が困難な場合は個人データの提供を停止)
- 日本と同等の水準国

情報提供の粒度

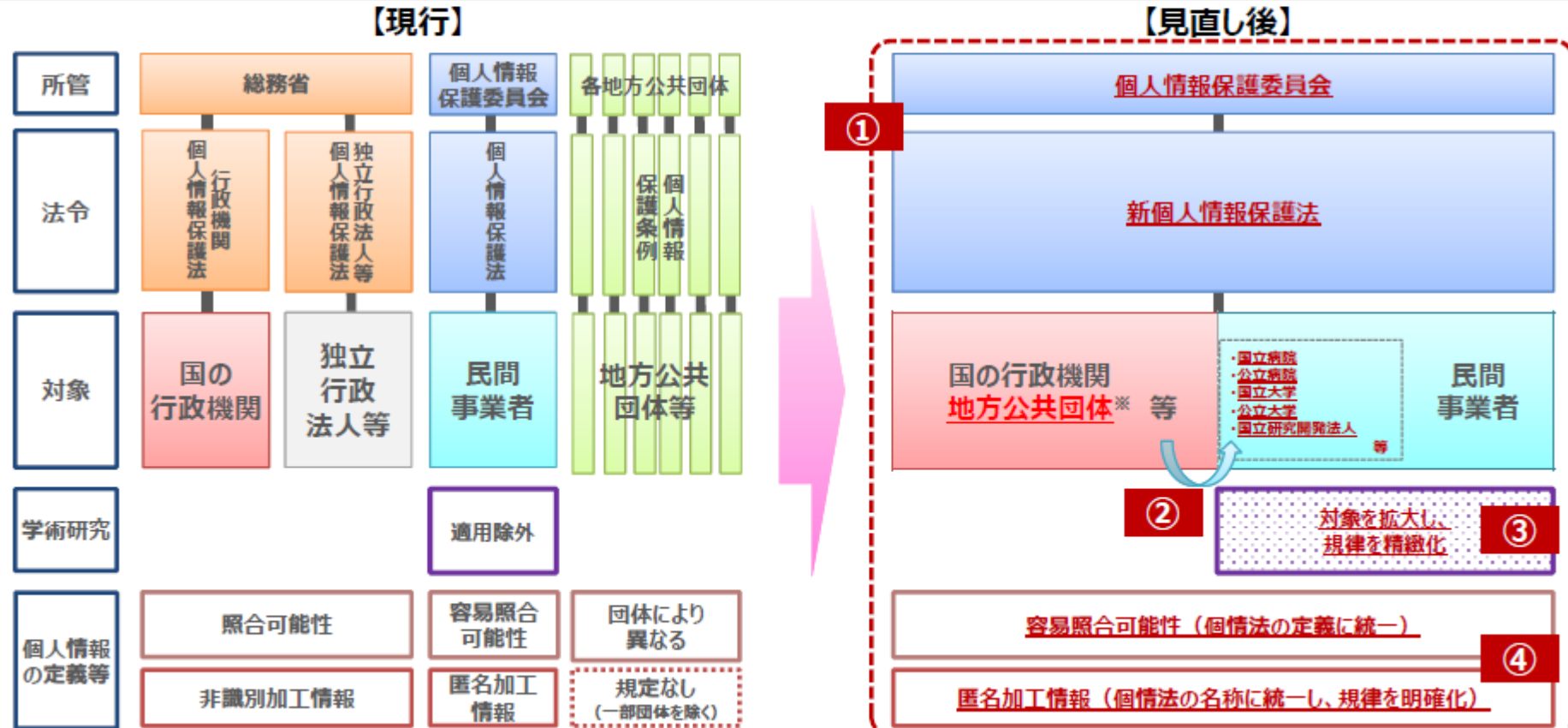
- 「移転先国における個人情報の保護に関する制度」については、網羅的な調査を求めるものではなく、あくまで本人の予見可能性を高める趣旨から、我が国の個人情報保護法との本質的な差異等、必要最低限の内容・粒度を想定
 - ✓ 「我が国の個人情報保護法と同様の法令が存在するが、〇〇に関する義務が存在しない点で大きく異なる」
 - ✓ 「APEC 越境プライバシールール（CBPR）加盟国であり、我が国とほとんど同様の個人情報保護法制が存在する」
 - ✓ 「個人情報保護法制が存在するものの、政府による個人データのアクセスについて、特段の制限がみられない」 等
- 一般的な注意力をもって確認をすればOK
 - 外国とは、サーバーの位置ではなく、当該運営事業者の法人格として登記された外国

施行日

- 全面施行： 令和4年4月1日
- オプトアウト規定に係る経過措置： 令和3年10月 1 日
- 法定刑引上げ： 令和 2 年12月12日

令和3年個人情報保護法改正案

- ① 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の3本の法律を1本の法律に統合するとともに、地方公共団体の個人情報保護制度についても統合後の法律において全国的な共通ルールを規定し、全体の所管を個人情報保護委員会に一元化。
- ② 医療分野・学術分野の規制を統一するため、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用。
- ③ 学術研究分野を含めたGDPRの十分性認定への対応を目指し、学術研究に係る適用除外規定について、一律の適用除外ではなく、義務ごとの例外規定として精緻化。
- ④ 個人情報の定義等を国・民間・地方で統一するとともに、行政機関等での匿名加工情報の取扱いに関する規律を明確化。



＜地方公共団体の個人情報保護制度に求められるもの＞

1 社会全体のデジタル化に対応した「個人情報保護」と「データ流通」の両立

※ いわゆる「2000個問題」

- ① 団体ごとの規定・運用の相違が、データ流通の支障となりうること
- ② 条例がないなど、求められる保護水準を満たさない団体があること等への問題提起がなされている

2 個人情報保護に関する国際的な制度調和と我が国の成長戦略への整合

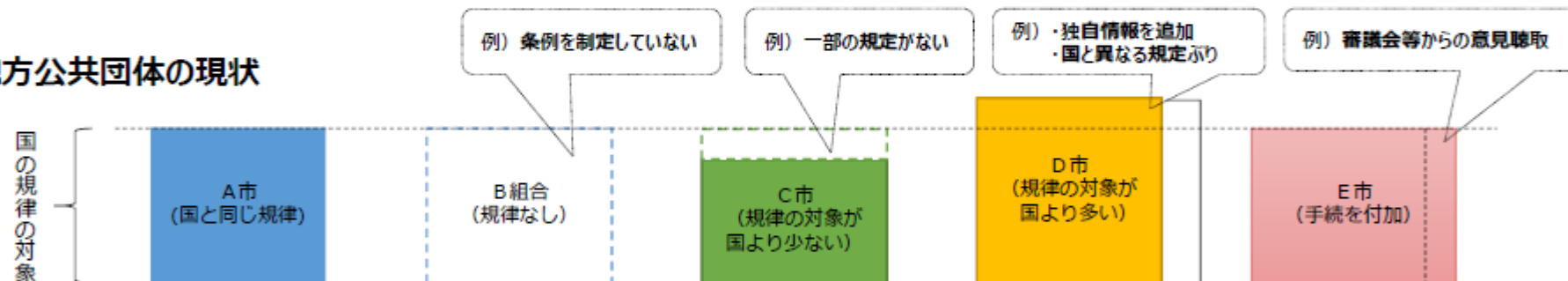
- 例) ・EUにおけるGDPR（一般データ保護規則）十分性認定
 ・G20大阪首脳宣言におけるDFFT（信頼ある自由なデータ流通）

＜改正の方向性＞

- 「個人情報保護」と「データ流通」の両立に必要な全国的な共通ルールを法律で設定
- 法律の確かな運用を確保するため、国がガイドラインを策定
- その上で、法律の範囲内で、必要最小限の独自の保護措置を許容

- 例) ・「要配慮個人情報」として保護する独自の情報を追加
 ・保護のため、必要な場合に限り審議会等からの意見聴取手続きを規定

○ 地方公共団体の現状



○ 共通ルール化後



※医療・学術分野については、国の組織同様、民間規律を適用する。

※審議会等の役割は、個別事案に関する審議から、定型事例についての事前ルールの設定や、制度の在り方に関する調査審議に主な役割が移行。

趣旨

- 社会全体のデジタル化に対応した「個人情報保護」と「データ流通」の両立が要請される中、
 - ・団体ごとの個人情報保護条例の規定・運用の相違がデータ流通の支障となりうる
 - ・求められる保護水準を満たさない団体がある 等の指摘。（いわゆる「2000個問題」）
- 独立した機関による監督等を求めるEUにおけるGDPR（一般データ保護規則） 十分に認定など国際的な制度調和とG20大阪首脳宣言におけるDFFT（信頼ある自由なデータ流通）など我が国の成長戦略への整合の要請。
- こうした課題に対応するため、地方公共団体の個人情報保護制度について、全国的な共通ルールを法律で規定するとともに、国がガイドライン等を示すことにより、地方公共団体の的確な運用を確保。

概要

① 適用対象

- ・地方公共団体の機関及び地方独立行政法人を対象とし、国と同じ規律を適用
- ・病院、診療所及び大学には、民間部門と同じ規律を適用
- ※④、⑤、⑥に係る部分は除く

② 定義の一元化

- ・個人情報の定義について、国・民間部門と同じ規律を適用
- 例：容易照合可能性、個人識別符号、要配慮個人情報 等

③ 個人情報の取扱い

- ・個人情報の取扱いについて、国と同じ規律を適用
- 例：保有の制限、安全確保措置、利用及び提供の制限 等

④ 個人情報ファイル簿の作成・公表

- ・個人情報ファイル簿の作成・公表について、国と同じ規律を適用
- ※個人情報ファイル簿の作成等を行う個人情報ファイルの範囲は国と同様（1,000人以上等）とする
- ※引き続き、個人情報取扱事務登録簿を作成することも可能とする

⑤ 自己情報の開示、訂正及び利用停止の請求

- ・開示等の請求権や要件、手続きは主要な部分を法律で規定

⑥ 匿名加工情報の提供制度の導入

- ・匿名加工情報の提供制度（定期的な提案募集）について、国と同じ規律を適用
- ※ただし、経過措置として、当分の間、都道府県及び指定都市について適用することとし、他の地方公共団体は任意で提案募集を実施することを可能とする

⑦ 個人情報保護委員会と地方公共団体の関係

- ・個人情報保護委員会は、地方公共団体における個人情報の取扱い等に関し、国の行政機関に対する監視に準じた措置を行う
- ・地方公共団体は、個人情報の取扱い等に関し、個人情報保護委員会に対し、助言その他の必要な支援を求めることが可能
- 例：個人情報の提供を行う場合、匿名加工情報の作成を行う場合 等

⑧ 施行期日等

- ・施行期日は、地方公共団体において必要な準備に十分配慮して設定
- ・地方公共団体は、法律の施行に必要な条例を制定 例：手数料、処理期間 等
- ・国は、制度の適正かつ円滑な実施を確保するため、地方公共団体の準備等について必要な助言（ガイドライン等）を行う

※地方公共団体が条例で定める独自の保護措置について

- ・特に必要な場合に限り、条例で、独自の保護措置を規定
- ・条例を定めたときは、その旨及びその内容を個人情報保護委員会に届出

施行日

- 公布から1年以内
- 地方公共団体関係は公布から2年以内

衆議院附帯決議(第204回国会閣法第30号)①

四 デジタル社会の形成を図るための関係法律の整備に関する法律の施行に関し、以下の事項について配慮すること。

1 個人の権利利益の保護を図るため、自己に関する情報の取扱いについて自ら決定できること、本人の意思に基づいて自己の個人データの移動を円滑に行うこと、個人データが個人の意図しない目的で利用される場合等に当該個人データの削除を求めること及び本人の同意なしに個人データを自動的に分析又は予測されないことの確保の在り方について検討を加え、必要な措置を講ずること。

2 地方公共団体が、その地域の特性に照らし必要な事項について、その機関又はその設立に係る地方独立行政法人が保有する個人情報の適正な取扱いに関して条例を制定する場合には、地方自治の本旨に基づき、最大限尊重すること。また、全国に適用されるべき事項については、個人情報保護法令の見直しを検討すること。

衆議院附帯決議(第204回国会閣法第30号)②

3 行政機関等が保有する個人情報等の目的外での利用又は第三者への提供については、その要件である「相当の理由」及び「特別の理由」の認定を、厳格に行うこととし、行政機関等が行った判断の適否を、個人情報保護委員会が監視すること。

4 行政機関等が個人情報を利用する際、個人が自己の情報の利用状況を把握できる仕組みについて、情報通信技術の進展を踏まえた見直しを検討すること。

5 個人情報保護委員会による行政機関等の監視に当たっては、資料の提出及び実地調査を躊躇なく行うとともに、必要があれば勧告や報告の要求を遅滞なく行うことにより、監視の実効性を確保すること。

衆議院附帯決議(第204回国会閣法第30号)③

6 大量に個人情報を保有している事業者が我が国の個人情報に関する法令を遵守するよう徹底するとともに、必要な場合には立入検査、報告徴収等の権限を躊躇なく行使し、遵守状況について監視すること。

7 個人情報保護委員会が民間部門と公的部門における個人情報保護に関する業務を所掌することに鑑み、個人情報保護委員会の体制強化を図ること。

8 学術研究目的における個人情報の取扱いについては、個人の権利利益を不当に侵害する場合は個人情報の取扱いに係る制限の適用除外とならないことに鑑み、要配慮個人情報を含む個人情報の適正な取得や提供等の保護の取組を強化すること。